# AES2 Conference Attendee Feedback

At the conclusion of the Second AES Candidate Conference (AES2), after all of the presentations and discussions had been completed, NIST passed out a conference feedback form to the attendees, which contained the following information:

"In the September 1998 Federal Register notice that announced the Round 1 evaluation period for the AES, NIST asked for official comments regarding which candidate algorithms should be selected for Round 2. Specifically, commenters were asked to identify which FIVE or fewer of the AES candidate algorithms should be selected for Round 2, and identify which algorithms should NOT qualify for Round 2. In that spirit, AES2 attendees may *optionally* respond to the following question, to give NIST and the public a "sense" of the opinions of the conference attendees. The results will not necessarily be an accurate reflection of the overall opinions of the cryptographic community and others interested in the AES development effort who did not attend AES2. NIST is still accepting official comments on the Round 1 AES candidates until April 15, 1999. Please see www.nist.gov/aes for details. **This is an ANONYMOUS, unofficial feedback form. Information collected on this form shall be made publicly available, including a summary of results at the Fast Software Encryption workshop.**

For each of the Round 1 algorithms listed below, please CIRCLE the number of your choosing, in response to the question: **"Should NIST select AES candidate algorithm X as a candidate for Round 2 evaluation?"** In addition, please include a short justification for your response. (Please limit the number of "1" choices to FIVE OR LESS.)

| | | | |
|---|---|---|---|
| Key: | **1** | **=** | **YES – it should definitely be selected for Round 2.** |
| | **2** | **=** | **I do not know – it could go either way.** |
| | **3** | **=** | **NO – it should NOT be selected for Round 2.** |

[A table was also provided, which listed all 15 algorithms, the selection number 1, 2, 3, and space to provide a brief rationale for the numerical selection of each algorithm. The results obtained from this feedback form are presented in the following table, which was presented by Miles Smid at the Rump Session of the Sixth Fast Software Encryption Workshop on March 25 1999.]

| | No Response | YES (1) | ? (2) | NO (3) | YES - NO | RANK |
|---|---|---|---|---|---|---|
| Rijndael | 7 | 77 | 19 | 1 | 76 | 1 |
| RC6 | 4 | 79 | 15 | 6 | 73 | 2 |
| Twofish | 9 | 64 | 28 | 3 | 61 | 3 |
| MARS | 5 | 58 | 35 | 6 | 52 | 4 |
| Serpent | 6 | 52 | 39 | 7 | 45 | 5 |
| E2 | 11 | 27 | 53 | 13 | 14 | 6 |
| CAST-256 | 12 | 16 | 58 | 18 | -2 | 7 |
| SAFER+ | 13 | 20 | 47 | 24 | -4 | 8 |
| DFC | 12 | 22 | 43 | 27 | -5 | 9 |
| Crypton | 14 | 16 | 43 | 31 | -15 | 10 |
| DEAL | 10 | 1 | 22 | 71 | -70 | 11 |
| HPC | 12 | 1 | 13 | 78 | -77 | 12 |
| MAGENTA | 9 | 1 | 10 | 84 | -83 | 13 |
| Frog | 11 | 1 | 6 | 86 | -85 | 14 (t) |
| LOKI97 | 10 | 1 | 7 | 86 | -85 | 14 (t) |

(A total of 104 out of the 180 conference attendees completed the optional feedback form.)